学校编码：10384　　分类号____密级_____
学号：X2009230333　　UDC_____

硕　士　学　位　论　文

基于角色访问控制的组织机构权限系统的设计与实现

Design and Implementation of Organization Permission System Based on RBAC

廖 庆 文

指导教师姓名：　王备战　　教授
专　业　名　称：　软　件　工　程

论文提交日期：　　年　　月
论文答辩时间：　　年　　月
学位授予日期：　　年　　月

答辩委员会主席：_____
评　　阅　　人：_____

2011 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

访问控制技术是对资源权限控制的一种安全机制，基于角色的访问控制也是近几年研究的热点。由于其在安全和管理上相对于传统的访问控制技术都具备极大的优势，因此替代和补充传统访问控制机制引起了广泛关注和重视。

基于角色的访问控制的核心核心思想是，建立角色作为用户和资源之间的桥梁，使用户无法直接对资源进行访问，而是需要通过角色的指定来实现。角色是根据用户在企业中的职权和责任进行设定，与企业中的实际组织机构相吻合，而资源在管理上只与角色相关联，使得资源与用户在逻辑上相分离，减少了授权管理复杂性，降低了管理开销，并增强了权限控制的灵活性。

本文首先介绍了访问控制技术的内容和发展情况，详细描述了访问控制技术中三个典型技术“自主访问控制”、“强制访问控制”和“基于角色访问控制”，并详述了三个技术的特点。通过对前两种技术缺陷的分析，引出角色访问控制，并阐述系统使用角色访问控制的必要性，接着再对企业组织机构的表现形式进行详细介绍，通过分析和比较，说明了企业的适用形式。

其次，通过分析企业开发组织机构权限系统的必要性与可行性，再对系统开发的需求进行描述，为系统的设计于实现奠定基础。

最后，结合基于角色的访问控制以及组织机构表现形式，对系统进行详细设计与实现，并对系统操作方式进行详细的演示。该系统实现了企业组织机构权限管理，并将其运用到实际企业中，提升了企业的组织管理的效率，同时减少了管理成本。

关键词：访问控制；组织机构；RBAC

Abstract

Access control technology is one of the security mechanisms of resource access control. In recent years, the Role Based Access Control has became a hot topic which has great advantage in safety and management compared with traditional one, therefore, as the substitutes and complements of traditional access control technology, it has aroused widespread attention.

The core idea of Role Based Access Control is to establish a role as a bridge between the user and the authority which made the user couldn't access to the resource directly but through the one designated by the role. The role was set according to user's authority and responsibility which conform to the actual organization of an enterprise. However, authority associated only with role in management which separated authority and user logically, reduce both the complexity of authorized management and the overhead of management, and enhance the flexibility of authority control.

This dissertation firstly introduced the content and the development situation of access control technology, and the three typical technologies of access control technology also their respective characteristics were described in details. The three typical technologies of access control technology are Discretionary Access Control, Mandatory Access Control and Role Based Access Control, and Role Based Access Control was draw forth through analyzing the defects of the former two technologies to state the necessity of systematic use of it, then a detailed account of the manifestation of enterprise organization was given. And through the analysis and comparison, this dissertation will explain each applicable form for the various kind of enterprise.

Secondly, with analyzing the necessity and feasibility of developing enterprise organization's privileged system, this dissertation will also describe the need of system development to forming the foundation for the design of system.

Lastly, combing Role Based Access Control and the manifestation of enterprise organization, this dissertation carries out a particular design and implementation, also makes detailed demonstration of the system operation mode. With the realization of enterprise organization right management, this system was used in a particular way which improves efficiency of organization management and reduces management cost at the same time.

Key Words: Access Control; Organization; RBAC

目 录

Contents

第一章 绪 论

1.1 研究背景

随着计算机技术的快速发展，计算机的应用领域也得到了广泛的普及。然而，企业当中为了保证信息系统数据的安全性，明确用户的责任，合理控制用户对数据资源的访问权限，也变得尤为重要与迫切。

访问控制技术，是维护信息系统的安全，以及保护系统资源的重要手段。目前主流的访问控制策略主要有三种[1]：自主访问控制（Discretionary Access Control，DAC）、强制访问控制（Mandatory Access Control，MAC）和基于角色的访问控制（Role Based Access Control，RBAC）。

DAC 和 MAC 是美国军方于 1985 年提出可信计算机系统的评估准则（Trusted Computer System Evaluation Criteria TCSEC）中描述的两种安全策略自主访问控制，这两种都属于传统的访问控制策略。传统的访问控制机制是对系统中的所有用户进行直接权限管理，权限操作复杂，授权方式也不灵活，很难满足大型企业的管理信息系统的发展需求。美国国家标准化和技术委员会（National Institute of Standards and Technology，NIST）的 Ferraiolo 等人在 90 年代提出了基于角色的访问控制。

基于角色访问控制引入了角色的概念，通过角色，将用户和系统资源相分离。通过角色再将用户和系统资源相关联，给用户分配适当的角色，以授予对不同系统资源的访问权限。达到用户和访问权限的逻辑分离，降低了授权管理的复杂性，并减少管理上的开销。

RBAC 具备的灵活性，方便性和安全性，使其得到了许多企业的重视，并在许多大型数据库系统的权限管理中得到了广泛的应用。

组织机构以职责和权限的形式定义了企业成员、企业各个部门的作用与任务，同时提供灵活的结构与不同的企业或企业中不同的组织结构相适应。对于以上问题，RBAC 无疑是现今最适合的一种访问控制模型。

1.2 国内外研究现状

随着信息系统的不断庞大和日益复杂化、多元化，经典的 DAC 和 MAC 已经无法满足日益增长的安全需求。因此，从 20 世纪 80 年代开始，先后有人提出了 Bell-Lopadula 模型、Take-Grant 模型、Biba 模型等访问控制模型，但是都不能从

根本上解决问题[2]。之后，角色的概念被提出来，通过给用户分配角色，使用户获得相应权限，进而产生 RBAC 模型。

1992 年，Honghai Shen 等首次提出面向协作系统的访问控制模型[3]，该模型在经典的 Lampson 模型的基础上进行拓展，建立角色继承、客体继承、权限继承等对象继承关系，同时，依据客体继承关系建立满足主体协作需求的访问控制策略。同年由 David Ferraiolo 和 Rick Kuhn 提出的模型，称为 Ferrailol-Kuhn92 模型是 RBAC 第一个模型。自 1993 年以来，访问控制方面的研究人员还提出了其他访问控制模型。Ravi Sandhu 教授和他的学生提出了基于任务的访问控制(Task Based Access Control，TBAC)模型。1994 年，David Ferraiolo 和 Rick Kuhn 在《Role 一 BasedAccessControl》一文中首先给出了基于角色的访问控制概念，并且在综合了大量的实际研究之后，率先给出基于角色的访问控制模型框架和 RBAC 模型的形式化定义，指出 RBAC 模型实现的最小特权原则 (Least Privilege)和职责分离原则(Separation of Duty)[4]。该模型给出一种集中式管理的 RBAC 管理方案。同年，华中理工大学(现华中科技大学)的马建平给出了“一种无干扰的访问控制模型”[5]。Matunda_Nyanchama 和 Sylvia Osborn 在研究了 RBAC 模型中角色继承关系和角色权限指派，形式化的给出了角色管理的一系列算法[6]。他们指出：他们提出的角色组织结构足够基本，能够模拟其他形式的权限模型，比如树状层次结构（Hierarchies）和权限图（Privilege Graphs）。1996 年，美国乔治梅森大学的 R.Sandhu1996 年提出了著名的 RBAC96 模型[7]，并在 IEEE Computer 期刊上发表的经典文献“Role-Based Access Control Models”中进行具体阐述，该模型完整地描述了 RBAC 基本框架，根据需要将传统 RBAC 模型拆分成四种嵌套的模型并给出形式化定义，较大地提高了系统灵活性和可用性。1997 年，他们更进一步提出一种分布式 RBAC 管理模型 ARBAC97[8]，在 ARBAC97 中角色分为常规角色和管理角色，二者互斥，管理角色具有等级结构和权限继承。访问权限也分为常规权限和管理权限，也是互斥的。ARBAC99 首次引入了静态和非静态的用户和权限的概念，并且先决条件被引入到 ARBAC 的回收机制中，ARBAC 的表达能力得到了加强，提高了对基于角色的访问控制系统的管理能力。ARBAC97 和 ARBAC99 都给 RBAC 系统的管理问题提供了可行的解决途径，能够很好地将安全策略的集中控制和分散管理相结合，实现基于 RBAC 模型基础上的分布式管理[9]。2002 年，Oh 和 Sandhu 等人又提出了 ARBACOZ 模型。它保留了 ARBAC97 模型的主要特

征，增加了新的概念“组织结构”。采用新独立于角色或角色层次的用户和权限库和一个自底向上的权限一角色分配管理模式，克服了 ARBAC97 模型的不足[10]。

在国内，许多研究人员也先后在 RBAC96 基础上进行，并提出新模型，包括乔颖等提出的新型 RBAC 模型[11]，胡和平等提出的基于业务工作流和角色的访问控制模型[12]，以及在 RBAC97 模型的基础上，陈林等提出的基于角色的多级访问控制模型[13]等。李成揩等人提出了基于角色的 CSCW 系统访问控制模型[14]，对数据、操作、权限、角色和用户等要素及其相互间的关系进行形式化描述。安晓江等人对 PMI 系统中的 RBAC 策略的管理进行了研究，提出将 PMI 系统的策略进行实现，侧重于策略修改的形式化描述[15]。

1.3 论文研究意义和内容

随着企业信息化的发展，传统的访问控制策略已经不再适合企业的信息资源管理。用户的增加和系统功能的扩充，大大增加了系统的管理难度，安全性也随之降低，然而用传统的访问控制策略解决这些问题，无疑会增加企业的管理费用。运用目前而言最优秀的访问控制策略 RBAC，进行管理系统设计，是目前企业的当务之急。用 RBAC 来替换传统的访问控制模式，不仅降低了授权管理的复杂性，而且还可以减少管理的费用，因此，对它的研究和应用，具有重要的现实意义。

本论文主要涉及访问控制的理论研究与组织机构的应用相结合。通过研究访问控制的基本模型，引出 RBAC，并掌握其“用户——角色——资源”的核心实质。

根据 RBAC 基本规则和完整性约束、结合实际组织机构的情况，设计并实现了基于角色访问控制的组织结构权限系统，方便授权管理，并具有一定扩展性。

1.4 论文组织结构

本文共分为五章，其组织结构如下：

第一章 绪论

介绍了访问控制技术的背景与国内外的发展现状，以及本论文的研究内容和研究意义。

第二章 相关技术介绍

详细介绍了当前比较流行的几种访问控制技术，DAC、MAC 和 RBAC，同时还介绍了组织机构的各种不同表现形式，以及各自的优缺点，并对它们进行了比较，为组织机构权限系统设计和实现提供理论基础。

第三章　系统分析

对组织机构权限系统开发的必要性和可行性进行了分析与介绍，同时对系统的需求进行了详细的说明，为系统开发做必要的准备。

第四章　系统设计与实现

通过对系统数据库设计、模块设计以及访问流程设计的介绍，并且展现系统的实现页面，进行说明系统是如何基于角色来达到访问控制的。

第五章　总结与展望

总结与展望部分，对本文的研究成果、系统的设计与实现做了一个总结，阐述了该系统存在的问题和不足，并对今后系统的改进提出了展望。

第二章 相关技术介绍

访问控制技术是在保障授权用户能够获取所需资源时，并同时拒绝非授权用户的安全机制。访问控制技术也是信息安全理论基础的重要组成部分。本章主要对访问控制技术的基本概念进行了概述，并对主要模型进行分析与阐述。

2.1 访问控制技术概论

访问控制技术是指主体依据某些控制策略或权限对客体本身或其他资源进行的不同授权访问。它是确保信息系统安全的重要措施，其基本目标是防止非法用户进入系统以及合法用户对系统资源的非授权使用。为了达到该目标，用户身份认证是实现访问控制的前提。控制未授权用户进入系统，各种访问控制策略都是以此为基础的，从而实现对合法用户在系统中的行为的控制和规范，进而保证系统的信息资源的合法受控使用。

一般而言，一个完整的访问控制系统包括以下三个要素：

1、主体(Subject)：执行访问、存取操作的主动方。通常指用户或任何主动发出访问操作请求的智能体，包括程序、进程、服务等。

2、客体(Object)：包括所有受访问控制保护的资源。针对不同的应用背景，其具有相当广泛的定义，比如在办公自动化系统中可以是打印文件，在数据库里可以是表中的记录，而在 web 应用系统中则可以是页面。

3、授权策略：一套确定主体对客体是否拥有访问权限的规则，其是访问控制的根本。在一定的授权策略下，得到对该资源授权的用户就是该资源合法用户，否则为不合法用户。

在访问控制模型中既定义了主体、客体，也定义了主体对客体的访问是如何表示和操作的，授权策略的表达能力和灵活性受访问控制模型的影响。目前被大家广泛接受的主流访问控制模型主要有以下三种： DAC、 MAC 和 RBAC。其中 DAC 和 MAC 作为比较传统的访问控制方式，已得到普遍应用，而基于角色的访问控制则是在最近十多年才逐渐发展起来的策略。下面将对这三种访问控制模型及其优缺点进行逐一分析，并且着重分析在本论文所使用的基于角色的访问控制模型[16]。

2.2 访问控制模型

2.2.1 自主访问控制模型

自主访问控制，称其为自主访问控制是因为在 DAC 中，一个拥有一定访问权限的主体可以直接或间接地将权限传给其他主体[17]。它是一种常用的访问控制方式，基于对主体或主体所属的主体组的识别来限制对客体的访问，这种控制是自主的。自主是指主体能够自主的(可能是间接的)将访问权或访问权的某个子集授予其他主体。换言之，自主访问控制是由拥有资源的用户自己决定其他一个或一些主体可以在什么程度上访问哪些资源[18]。

自主访问控制是一种比较宽松的访问控制，一个主体的访问权限具有传递性。比如大多数交互系统的工作流程是：用户登陆，登录成功后就启动某个进程为该用户做某项工作，该进程就继承了该用户的属性，包括访问权限。该权限的传递可能会给系统带来安全隐患，某个主体通过继承其他主体的权限而得到了它本身不应具有的访问权限，就可能破坏系统的安全性。这同时也是自主访问控制方式的缺点。

为了实现完整的自主访问系统，访问控制矩阵内的内容必须以某种形式进行保存和管理。如果把整个矩阵保存下来，不仅给实现带来不便，而且效率较低。

访问控制表(Access Control List，ACL)是基于访问控制矩阵中列的自主访问控制。它在一个客体上附加一个主体明晰表，表示各个主体对这个客体的访问权限。明细表中的每一项都包括主体的身份和主体对这个客体的访问权限。

在实际的多用户系统中，用户可以根据部门结构或者工作性质分为有限的几类。一般而言，一类用户使用的资源基本相同。因此，可以将一类用户归为一组，分配组名，简称“GN”访问是可以按照组名判断。通配符“*”可以代替任何组名或者主体标识符。此时，访问控制表中的主体标识为：主体标识=ID.GN，其中，ID 表示主体标识符，GN 则表示主体所在组的组名。

在访问控制表中还需要考虑缺省问题。缺省功能的设置方便用户的使用，同时也避免了许多文件泄露的可能。最基本的，当一个主体生成一个客体时，该客体的访问控制表中对应生成者的表项应该设置成缺省值，比如具有读、写和执行权限。另外，当某一个新的主体第一次进入系统时，应该说明它在访问控制表中的缺省值，比如只有读的权限。

访问能力表是最常用的基于行的自主访问控制。能力(capability) 是为主体提供的、对客体具有特定访问权限的不可伪造的标志，它决定主体是否具有访问客体的权限以及访问客体的方式。主体可以将能力转移给为自己工作的进程，在进

程运行期间，可同时进行能力的添加或者修改。能力的转移不受任何策略的限制，使得对于特定的客体无法确定所有有权访问它的主体。因此，访问能力表无法实现完备的自主访问控制，而访问控制表则可以实现。利用访问能力表实现的自主访问控制系统不是很多，其中只有少数系统试图通过增加其他措施实现完备的自主访问控制。

能力机制的最大特点是：能力的拥有者可以在主体中进行转移能力。在转移的能力当中有一种“转移能力”，它允许接受能力的主体继续转移能力。比如，进程 X 将某个能力的拷贝转移给进程 Y，Y 又将能力的拷贝传递给进程 Z。如果 Y 不想让 Z 继续转移这个能力，就在转移给 Z 的能力拷贝中去掉转移能力，这样 Z 就不能转移能力了。主体为了在能力取消时从所有主体中彻底清除自己的能力，需要跟踪所有的转移。

2.2.2 强制访问控制模型

自主访问控制的最大特点是自主，即资源的拥有者对资源的访问策略具有决策权，因此是一种限制比较弱的访问控制策略。这种方式给用户带来灵活性的同时，也带来了安全隐患[18]。

在一些系统中，需要更加强硬的控制手段，强制访问控制就是其中的一种机制。顾名思义，MAC 是“强加”给访问主体的，即系统强制主体服从访问控制策略。MAC 是根据客体的敏感级别和主体的许可级别进行限制主体对客体的访问[19]，达到控制效果。

MAC 中客体和主体被分配了不同的安全级别，比如绝密级、机密级、秘密级和无密级。不同级别标记了不同重要程度与能力的实体。不同级别的主体对不同级别的客体的访问是在强制的安全策略下实现的，而且这些安全属性不能被修改。系统通过比较主体和客体的安全属性决定主体对客体的操作可行性。

在强制访问控制机制中，将安全级别进行排序，如按照从高到低排列，规定高级别可以单向访问低级别，也可以规定低级别可以单向访问高级别。这种访问可以是读，也可以是写或修改。

1、保障信息完整性策略

为了保障信息的完整性，低级别的主体可以读高级别客体的信息(不保密)，但低级别的主体不能写高级别的客体(保障信息完整)，因此采用的是上读 / 下写策略。即属于某一个安全级的主体可以读本级和本级以上的客体，可以写本级和本